Integral domains $R$. (with no zero divisors)

Factoring in $R$.

Why factorization useful?

Ex: $\sqrt{2}$ irrational

pf: If $\sqrt{2} = \frac{p}{q}$. $\underbrace{(p,q)}=1$. $p, q$ integer. coprime.

largest common divisor.

$$2q^2 = p^2.$$ 2 prime.

$2 | p$, $p = 2k$.

$q^2 = 2k^2 \Rightarrow 2 | q$. Contradiction.

$\mathbb{Z}$. $(p)$ $p$ prime give all the maximal ideals prime.

---

Terminology: $1 = uu^{-1}$.

① $u$ is a unit $\Leftrightarrow$ $(u) = (1) = R$. unit ideal.

② $a$ divides $b$, i.e. $b = ac$ for some $c$.

$a, b \neq 0$ $\Leftrightarrow$ $(b) \subset (a)$.

③ $a$ is a proper divisor of $b$.

$a, b \neq 0$

i.e. $b = ac$. neither "$a$" nor "$c$" is a unit.

$(\Leftarrow)$ $(b) \subsetneqq (a) \subsetneqq (1)$

$c$ is not a unit. $a$ not a unit.

$(b) = (a)$ means $b = ac$. $a, b, c, d \in R$

$a = b \cdot d$.

$b = b \cdot cd \Rightarrow cd = 1$.

④ $a, b \neq 0$. $a, b$ associates $(\Leftarrow)$ $(a) = (b)$.

i.e. $a = bc$

for some unit $c$.

⑤ $a \neq 0$. $a$ irreducible if $a$ is not unit.

$a$ not a unit.

$a$ has no proper divisor.

$(\Leftarrow)$ $(a) \subsetneqq (1)$

No principal ideal $(c)$

s.t. $(a) \subsetneqq (c) \subsetneqq (1)$

$(a) \neq (1)$ and $(a)$ is maximal (under inclusion) in principal ideals.

(b) $p$ is a prime element (not a unit)

if $p$ divides $ab$, then $p$ divides $a$ or $b$

$\iff ab \in (p) \Rightarrow a \in (p)$ or $b \in (p)$

$\iff R/(p)$ is an integral domain.

$\iff (p)$ is prime ideal.

---

Defn (PID) Principal ideal domain $R$.

every ideal of $R$ is a principal ideal $(a)$

Ex:

Recall that we proved $\mathbb{Z}$, $F(x)$ (where $F$ field) are PID. 1.1. deg.

we used DWR.

Defn: Euclidean domain $R$.

$R$ is an integral domain with size function $\sigma : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Such that

$\forall\, a, b \in R$, $b \neq 0$

$\exists\, q, r \in R$, s.t. $a = bq + r$

$r = 0$ or $\sigma(r) < \sigma(b)$.

Ex: $\mathbb{Z}$, $\sigma(a) = |a|$.

$F[x]$, $F$ field.

$\sigma(f) =$ degree of $f(x)$

---

Thm: Euclidean domain is PID

Pf: $I \neq (0)$. ideal of $R$, (Euclidean domain)

Consider $\{\sigma(r) \mid r \in I,\ r \neq 0\}$. has

a minimal value achieved by $\sigma(a)$, $a \in I$.

$\forall\, b \in I$, $\quad b = aq + r$.

① $r = 0$, $\quad b = aq$.

② $r \neq 0$, $\quad \sigma(r) < \sigma(a)$

Contradiction.

$$r = \underset{\substack{\cap \\ I}}{b} - \underset{\substack{\cap \\ I}}{aq} \in I.$$

Ex: $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$. $\quad i^2 = -1$.

$\sigma(a+bi) = |a|^2 + |b|^2 = |a+bi|^2$.

Let $\quad z_1 = a+bi \neq 0, \quad a \neq 0,\ b \neq 0.$

$\quad z_2 = c+di$

$z_2 = z_1 \cdot q + r$

( $q$ should be "close" to $\dfrac{z_2}{z_1}$ )

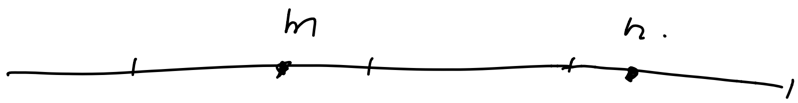
$\frac{z_2}{z_1}$ is a complex number

$$\frac{z_2}{z_1} = m + ni, \qquad m, n \in \mathbb{Q}.$$

because $\frac{z_2}{z_1} = (c + di) \cdot \frac{a - bi}{a^2 + b^2}$.

Choose $m_0, n_0 \in \mathbb{Z}$ such that $|m_0 - m| \leq \frac{1}{2}$.

$|n_0 - n| \leq \frac{1}{2}$.




$$q = m_0 + n_0 i.$$

$$q - \frac{z_2}{z_1} = (m_0 - m) + (n_0 - n)i.$$

$$\left|q - \frac{z_2}{z_1}\right|^2 = (m_0 - m)^2 + (n_0 - n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

$< 1$

$$\underbrace{|z_2 - q z_1|^2}_{= r \in \mathbb{Z}[i]} = \left|z_1\left(\frac{z_2}{z_1} - q\right)\right|^2$$

$$= |z_1|^2 \cdot \left|\frac{z_2}{z_1} - q\right|^2 < |z_1|^2.$$

$z_2 = q z_1 + r, \quad \sigma(r) < \sigma(z_1)$

$\mathbb{Z}[i]$ is PID

---

Defn (UFD) uniquely factorization domain.

① Factoring terminates.

$a \neq 0$, $a$ irreducible or not irreducible.

if not. $a = a_1 b_1$ $a_1, b_1$ not units.

$a_1 = c_1 d_1, \quad b_1 = c_2 d_2 \cdots$

After finite steps

$$a = a_1 a_2 a_3 \cdots a_n.$$

$a_i$ are irreducible.

② If $a = p_1 p_2 \cdots p_m$ $p_i$ irreducible.

$= q_1 q_2 \cdots q_n$ $q_i$ irreducible.

The irreducible factorization is unique

iff $m = n$ and after rearranging

$q_1 \cdots q_n$ suitably, $q_i$ is an associate

of $p_i$, i.e. $q_i = p_i u_i$, $u_i$ unit.

Example: $\mathbb{Z}$, $10 = 2 \cdot 5$ $\quad$ $-1$ unit in $\mathbb{Z}$

$$= (-5)(-2)$$

$$= (-2) \cdot (-5)$$

$\mathbb{Z}[i]$, $5 = (1+2i)(1-2i)$

$$= (2+i)(2-i)$$

$(2+i)$ and $(1-2i)$ are associates.

$$(2+i)\,i = (1-2i)$$

$i(i^3) = 1$ $\quad$ $i$ is a unit.

Goal: Euclidean domain $\Rightarrow$ PID $\overset{\text{Thm 1}}{\Rightarrow}$ UFD.

Thm 2: $R$ UFD, $R[x]$ also UFD.

~~Thm 1:~~ Lemma 1: $R$ integral domain. any prime element is irreducible.

Pf: $p$ prime element. if $p \mid ab$. then $p \mid a$ or $p \mid b$

if $p = ab$. $\Rightarrow$ $p \mid ab$. then

$p \mid a$ or $p \mid b$.

assume $p \mid a$, $a = p \cdot c$.

$p = p \cdot c \cdot b \Rightarrow cb = 1$. $b$ is a unit.

So $a$ is not a proper divisor.

---

Lemma 2. If $R$ is PID, then every irreducible element is a prime element.

pf: $p$ irreducible $\Rightarrow$ $(p)$ is maximal among principal ideals

$\Rightarrow$ $(p)$ is maximal ideal.

$\Rightarrow$ $R/(p)$ is a field

$\Rightarrow$ $(p)$ is a prime ideal.

PID: $R/(p)$ $p$ irreducible prime element. $\Rightarrow$ $R/(p)$ is a field.

Thm 1: i) Suppose factoring terminates in $R$. Then $R$ is UFD iff every irreducible element is a prime element.

ii) PID is UFD.

Pf: 1). " $\Leftarrow$ " $a = p_1 p_2 \cdots p_m$.

$= q_1 q_2 \cdots q_n$

Assume $m \le n$, Induction on $n$.

$n = 1$, $a = p_1 = q_1$

$n \geq 2$, $\quad q_1$ irreducible $\Rightarrow$ $q_1$ prime

$$\Rightarrow q_1(q_2 \cdots q_n) = p_1 \cdots p_m.$$

$q_1 \mid p_1(p_2 \cdots p_m)$, + $q_1$ prime

$\Rightarrow q_1$ divides $p_i$.

We can assume $q_1$ divides $p_1$,

and since $p_1$ is irreducible. $q_1$ is a unit

or associates with $p_1$.

$p_1, q_1$ are associates. $\quad p_1 = q_1 u_1$.

$$a = p_1 \cdots p_m = q_1 u\, p_2 \cdots p_m$$
$$= q_1 q_2 \cdots q_n.$$

$(u p_2) \cdots p_m = q_2 \cdots q_n$.

Induction on $n$ $\Rightarrow$ irreducible factorization is unique.

" $\Rightarrow$ " $p$ irreducible.

If $\underline{p} = ab. = \underbrace{p_1 \cdots p_m q_1 \cdots q_n}$.

$a = p_1 \cdots p_m$ irreducible factorizations.

$b = q_1 \cdots q_n$

$m+n=1$. $a$ or $b$ must be unit.

ii). We only need to prove factoring process terminates in PID.

If for some $a_0 = a, b_1, \ldots$

we have an infinite chain of factoring process

We get a chain of ideals.

$(a_0) \subsetneq (a_1) \subsetneq (a_2) \ldots$

Consider $\bigcup_{i=0}^{+\infty} (a_i) = I$, $I$ is an ideal.

$I = (a)$. $a \in (a_n)$. then $(a) \subset (a_n)$.

$I \subset (a_n)$. $(a_s) = (a_{n+1}) \cdots$

PID $\Rightarrow$ UFD.

---

Non Ex: $\mathbb{Z}[\sqrt{-5}] = \{ m + n\sqrt{-5} \mid m, n \in \mathbb{Z} \}$
subring of $\mathbb{C}$

is a UFD.

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Claim: $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible.
and the factorizations are different.

---

Determine units in $\mathbb{Z}[\sqrt{-5}]$.

Trick $|\cdot|^2$. If $z = m + n\sqrt{-5}$ is a unit.

$z \cdot w = 1$. $w = a + b\sqrt{-5}$.

$|z \cdot w|^2 = 1$. $(m^2 + 5n^2)(a^2 + 5b^2) = 1$.

$m^2+5n^2=1. \Rightarrow n=0,\ m=\pm 1.$

$\Rightarrow$ units in $\mathbb{Z}[\sqrt{-5}]$ are $\pm 1.$

2 irreducible because.

$2 = z \cdot w. \qquad z = m+n\sqrt{-5}$

$\qquad\qquad\qquad w = a+b\sqrt{-5}$

$$2^2 = |z|^2 \cdot |w|^2 \Rightarrow 4 = \underline{(m^2+5n^2)}\,\underline{(a^2+5b^2)}$$

$m^2+5n^2 = \underline{1.\ 2,}\ 4.$

$\Downarrow$

$n=0, \quad m^2 = 1, \text{ or } 4.$

$m = \underline{\pm 1}, \text{ or } \pm 2.$

$\Downarrow \qquad\qquad \perp$

units $\qquad$ associates to 2.

3 irreducible. $1+\sqrt{-5}$, $1-\sqrt{-5}$ irreducible.

Factorizations are different.

Thm 2: $R$, $R[x]$

UFD $\Rightarrow$ UFD